REMARKS

Claims 1-61 are pending in the application and stand rejected.

Rejection under 35 U.S.C §103

Claims 1-19, 22-37, 42-55 and 60-61 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,678,833 to Grawrock in view of U.S. Pat. No. 6,209,099 to Saunders and CCIMB-99-031. Applicants respectfully disagree, and address each of the Examiner's contentions below.

With respect to Applicants' claim 42, the Examiner alleges that Grawrock teaches presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity at col. 4 ll. 10-12 and 35-40, then goes on and "notes Grawrock teaches using the Trusted Platform Module (TPM) as the trusted 3rd party to provide target information metrics for verification by the trusted device either internally or externally." This is completely self-contradictory. The portions cited by the Examiner as disclosing the trusted device associated with the computer entity at col. 4 ll. 10-12 and 35-40 teach that "[t]he TPM 230 further responds to inquiry requests from a challenger. A 'challenger' may be any electronic device within the platform or even external to the platform." Grawrock also clearly teaches that it is the TPM that "performs a hash operation on the boot information to produce a boot identifier 330" (col. 3 ll. 59-61) and thus it is clear that the Examiner finds the TPM of Grawrock as corresponding to the claimed trusted device associated with the computer entity. Thus, if the TPM of Grawrock is the trusted device, how can it also be the "the trusted 3rd party to provide target information metrics for verification by the trusted device either internally or externally" as asserted by the Examiner? And if the TPM is not the trusted device, then what exactly is? The Examiner's allegation simply makes no sense, and also completely misconstrues the actual disclosure of Grawrock. Grawrock teaches nothing more than the fact that the TPM can respond to an inquiry request from an internal or external challenger. There is absolutely no further discussion whatsoever in Grawrock concerning the challengers, and what they may do with the responses received from the TPM in reply to their inquiry requests. Thus, contrary to the Examiner's assertion, there is no teaching nor hint in Grawrock of comparing the response of the

TPM with authenticated values, and the Examiner's repeated assertion that the "TPM is the trusted 3rd party" is, as explained above, simply nonsensical.

The Examiner further states that "Grawrock does not disclose explicitly about that particular trusted device," to which Applicants can only reply, Grawrock does not disclose **what** explicitly about **which** particular trusted device? With all due respect, Applicants simply do not understand what the Examiner intended to communicate by this statement.

The Examiner further continues "Saunders teaches the use of security ASIC as the trusted device." This flies completely against the Examiner's own prior statement that it is Grawrock that teaches the use of a trusted device to provide an integrity metric and which, as Applicants noted above, can clearly only be understood as being the TPM of Grawrock. If Applicants' understanding is not correct and the Examiner is not alleging that it is the TPM of Grawrock that anticipates the claimed trusted device, then Applicants request the Examiner to clearly and specifically identify the precise element of Grawrock that, according to the Examiner, "teaches presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity." Again, the sole portions of Grawrock cited by the Examiner, at col. 4 ll. 10-12 and 35-40, discuss exclusively the TMP, and clearly state that "[i]n response [to a challenge], the TPM 230 provides TPM services such as a digital signature featuring the boot block identifier 330, keying material, certificates and the like." Applicants submit that the Examiner unequivocally identifies the TPM of Grawrock as corresponding to the claimed trusted device, and thus the assertion that "Saunders teaches the use of security ASIC as the trusted device" is completely self-contradictory.

The Examiner finally opines that it would have been obvious to the skilled person "to combine the teaching of Saunders within the system of Grawrock because Saunders providing an effective method and system for testing one or more components of a data processing system in order to determine the authenticity of the tested component or components (Saunders: Column 1 Line 30-34)." It is hard to accept the Examiner's proffered "motivation" in light of the fact that Grawrock himself teaches that "the TPM can response to inquiry requests from a challenger to determine that the platform has been initialized and is trusted." Thus, why would the skilled

person be motivated to look further to Saunders "in order to determine the authenticity of the tested component or components" when Grawrock is already providing a way of doing so?

Applicants further note that the Examiner's assertion that "Saunders teaches the use of security ASIC as the trusted device" is incorrect in light of the plain disclosure of Saunders. The ASIC of Saunders does not calculate an integrity metric for the computer entity with which it is associated, but rather merely authenticates each hardware component of the computer entity by comparing a digital signature generated for that hardware component by the ASIC with a digital signature embedded in the component by its manufacturer (see, *e.g.*, col. 2 ll. 51-61 and col. 3 ll. 47-52). There is absolutely no information passed from the ASIC to any device external to the computer entity, and thus it cannot possibly be understood by the skilled reader as "presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device" as alleged by the Examiner, because (a) it does not calculate any integrity metrics, and (b) it does not present anything to the user. The Examiner's proffered reasoning that "the system and user as a whole is considered as a complete computer entity" defies all reason – how can a user of a computer be a part of that computer? Where in the art has the Examiner found reason to believe that a "complete" computer entity is comprised of a computer ***and its user***??? Referring to col. 3 ll. 47-50 of Saunders, as directed by the Examiner, does precious little to shed light upon the logic employed by the Examiner: "Validation of each plug-in card 13 is achieved by to comparison of the digital signature generated for that card by the cryptographic engine 19 with the digital signature embedded in the card using the appropriate `card x` key." Where does this passage teach presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device?

The Examiner further finds that Saunders teaches comparing at the user values in the integrity metric calculated for the entity by the trusted device at col. 3 ll. 47-50, and Grawrock teaches authenticated values provided for the entity by a trusted party, once again asserting that the TPM of Grawrock is the trusted 3rd party. Applicants have already addressed above, and in full, the fallacy of this view.

The Examiner finally acknowledges that Grawrock does not teach selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user

based on at least one value in the integrity metric calculated for the entity by the trusted device, but finds that CCIMB-99-031 teaches precisely this at p. 14 ¶3, p. 15 ¶1, p. 41 last ¶ and p. 48 last ¶, and opines that combining the teaching of this document within the system of Grawrock would have been obvious to the skilled person because it "teaches the prevention of system tampering by assigning a trusted assurance rating of the countermeasures, which gives grounds for confidence in their proper characteristics." Applicants submit that the Examiner reads far more in this document than it actually contains. At best, this document can be understood as teaching general principles to be employed when designing secure or trusted systems, all of which can be condensed to the overarching principle that the user needs to be reassured that security measures appropriate to the user's circumstances are in place. From a practical, enabling point of view, this document contains little indeed, and the very paragraphs referenced by the Examiner teach that different security levels in computer systems that are a target of evaluation (TOE) are determined in terms of different security functions, such as strength of encryption. There is nothing in common between this and the calculation of an integrity metric as claimed herein, and of passing such an integrity metric from the trusted device that calculated it to a requesting user, and the Examiner has made absolutely no showing as to how exactly one skilled in the art would go about combining the teaching of this document within the system of Grawrock. Furthermore, the Examiner's proffered motivation is once again completely lacking from the face of the documents themselves, as clearly set forth in MPEP §2142. As noted previously, Grawrock is concerned with making a computer more secure, and thus there is absolutely no reasonable expectation that one skilled in the art looking to practice Grawrock would feel compelled to dig for further security measures to implement, such as broadly alluded to in CCIMB-99-031.

Applicants respectfully remind the Examiner of the requirements posited by MPEP 2143.03 that "[t]o establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." (emphasis added) As fully set forth above, the Examiner has not made and indeed cannot make a *prima facie* showing that the newly cited art discloses each and every claimed

limitation, and the Examiner's strained attempt at forcing the disclosures of these three documents into a disjointed concoction is a very thinly disguised, and unsuccessful, attempt at using the claims themselves as a roadmap to stitching the prior art into something akin to the claimed invention. The Examiner's "reasoning" is full of self-contradictory, erroneous, and/or simply nonsensical statements which clearly indicate a complete lack of understanding of the invention and the art within which it arises on the part of the Examiner. Applicants have already spent significant resources and time attempting to educate the Examiner, and now strongly urge him to take the time and thoroughly read the claims, read the specification, and read the prior art documents in full before issuing the next Action. In view of all of the above, Applicants submit that claim 42 is in fact nonobvious and allowable and respectfully request the Examiner to reconsider and pass this claim to issue.

The Examiner further states "[a]s per claim 1, 6, 7 and 24, the claim limitations are met as the same reasons as that set forth in rejecting claim 42." Because Applicants have addressed in full the Examiner's rejection of claim 42 and shown it to be in error, they submit that claims 1, 6, 7 and 24 are allowable over the art for the same reasons as those set forth in proving the allowability of claim 42, and do not individually address these claims elsewhere herein but rather respectfully urge the Examiner to pass these claims to issue as well.

Claims 2-5 depend from claim 1, 8-23 depend from claim 7, claims 25-41 depend from claim 24, and 43-61 depend from claim 42. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 42, Applicants submit that claims 2-5, 8-23, 25-41 and 43-61 are also nonobvious and allowable and therefore are not individually addressed elsewhere herein.

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

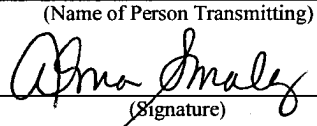
A Notice of Change of Correspondence Address is filed concurrently herewith. Kindly note the new Attorney Docket Number for this case.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

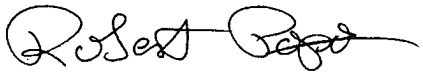
January 10, 2006
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)


(Signature)

1/10/06
(Date)

Respectfully submitted,



Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com